Da ist Adrenalin im Call.

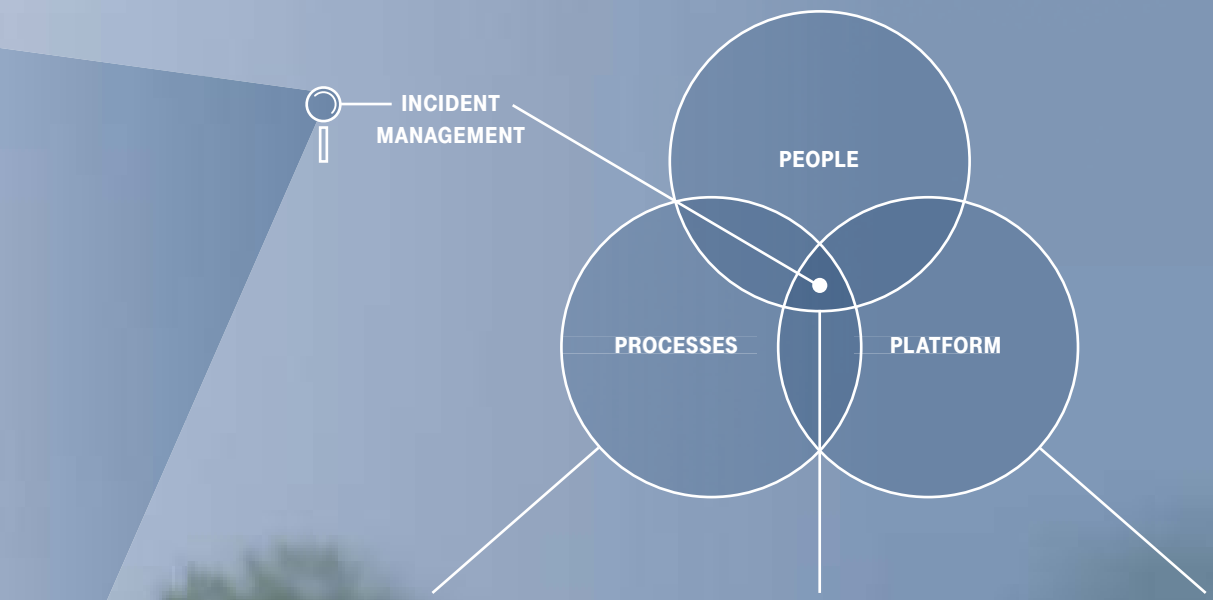
IM FALL EINES IT-INCIDENT ZÄHLT FÜR DEN KUNDEN JEDE MINUTE. FÜR DIE SCHNELLSTMÖGLICHE BEHEBUNG VON STÖRUNGEN UND DIE ZUVERLÄSSIGE IDENTIFIKATION DER URSACHEN STELLT T-SYSTEMS IHR GANZHEITLICHES QUALITÄTSMANAGEMENT REGELMÄSSIG AUF DEN PRÜFSTAND. IN MEHR ALS 500 „FIRE DRILLS“ (ERNSTFALL-SIMULATIONEN) JÄHRLICH TESTET DIE TELEKOM-TOCHTER DAZU DAS ZUSAMMENSPIEL IHRER MITARBEITER, PARTNER, PROZESSE UND PLATTFORMEN SOWIE DIE DAHINTERLIEGENDE LOGIK. SICHTBAR MACHT DAS ERGEBNIS STÄNDIGER ÜBUNG EIN BLICK AUF DAS INCIDENT MANAGEMENT. DOCH OB REAL ODER WIRKLICHKEITSNAH, IST DABEI KAUM MEHR ZU UNTERSCHEIDEN.

*‹**Text**› Klaus Rathje*

Foto: Thorsten Futh

QUALITÄT MANAGEN – ERFOLGE SICHERN.

Das ganzheitliche Qualitätsprogramm Zero Outage gewährleistet Kunden maximale Zuverlässigkeit in IT-Betrieb und Transitions-/Transformationsprojekten: kontinuierliche Überprüfung und Feinjustierung sämtlicher Leistungen und Systeme; permanente Weiterentwicklung von Prozessschritten. Ein definiertes 3-P-Konzept (Processes – People – Platforms) treibt Qualitätsmaßnahmen in alle Unternehmensebenen. Einheitlicher und einziger Maßstab: bestes Ergebnis für den Kunden.



DAS EINHALTEN KLAR DEFINIERTER PROZESSE BESCHLEUNIGT DIE TRANSPARENZ DER ERGEBNISSE UND ERMÖGLICHT JEDERZEIT EINE SCHNELLE (RE-)AKTION.

DISZIPLIN
Regelmäßige Incident-Übungen trainieren Reaktionsgeschwindigkeit und Notfallabläufe, überprüfen Disziplin und Prozesstreue interner Einheiten und Partner. Wöchentliche Ergebnisberichte münden in konkrete Verbesserungsmaßnahmen.

VIER-AUGEN-PRINZIP
Striktes Vier-Augen-Prinzip bei kritischen Themen gewährleistet Fehlerausschluss und Qualitätskontrolle.

DER MENSCH IM FOKUS – ZERO-OUTAGE-KULTUR DURCH (WEITER-)BILDUNG, VERHALTEN UND VERANTWORTUNG.

QUALITY ACADEMY
Die interne Trainings- und Portfolioplattform „Quality Academy" zertifiziert befristet mehr als 21 000 Mitarbeiter, verankert die Zero-Outage-Kultur und Process Compliance bei jedem Einzelnen jährlich neu.

TOPMANAGEMENT-ATTENTION
Wöchentliche Reviews involvieren die Führungsspitze in sämtliche Prozesse, kritische Projekte oder Betriebsstörungen und sichern so wettbewerbsdifferenzierende Topmanagement-Attention für a) schnelle Entscheidungsfähigkeit durch konzernweite Einbindung des Topmanagements inklusive Geschäftsführer bei Major Incidents, b) die Einhaltung aller wesentlichen Qualitätskennzahlen (KPI) und c) die Umsetzung konkreter Verbesserungsmaßnahmen.

AKTIVE KUNDENKOMMUNIKATION
Serviceschnittstelle bündelt die Kundenrückmeldung zur Ablaufoptimierung und hohen Prozesskorrespondenz mit den Geschäftserfordernissen der Unternehmen.

DIE TECHNISCH EINWANDFREIE UMSETZUNG IST EIN WESENTLICHER ERFOLGSFAKTOR.

HOCHVERFÜGBARE IT
Stabile, redundant-ausfallsichere IT-Infrastrukturen sorgen für hochverfügbare Systemlandschaften – Stichwort: TwinCore-Rechenzentren. Umfassendes Monitoring und regelmäßige Präventivtests aller Komponenten decken Überlastungen oder Defekte auf.

SUPPLIER-ZERTIFIZIERUNG
Ausweitung der Zero-Outage-Zertifizierung auf Lieferanten sichert bei Incident-, Problem- und Change-Management maximale IT-Verfügbarkeit Ende-zu-Ende.

Das sieht nicht gut aus – die Erstbeurteilung des GLIM entscheidet, welche Spezialisten Steffen Germersdorf beim Incident Management hinzuholt.

WER BEREITSCHAFT HAT, MUSS JEDERZEIT EINSATZBEREIT SEIN. So musste auch Steffen Germersdorf an einem der Feiertage im Mai „immer damit rechnen", dass das „rote Telefon" bei ihm klingelt. Der 31-Jährige ist eine der Stimmen des Global MoD Service, des internationalen Serviceteams von T-Systems, das sich um kritische IT-Ausfälle der Kunden kümmert. Dann koordinieren die Global Lead Incident Manager (GLIM) einen weltweiten Pool von 1000 Kollegen in verschiedenen „Rollen", die T-Systems mit ihrer Expertise 24 Stunden am Tag vorhalten kann, und pro Woche einen Kern von 140 Mitarbeitern, die als Manager-on-Duty (MoD) weltweit im Einsatz sind.

BERLIN, 10:57 UHR:
JOBWECHSEL IM HOMEOFFICE

Im Grunde sei sein Job so ähnlich wie bei der Feuerwehr. „Manchmal passiert tatsächlich nichts während einer Schicht, aber sobald ein Brand ausbricht, müssen alle sofort hellwach und präsent sein." Nur dass Germersdorfs zu löschende Feuer, um im Bild zu bleiben, in seiner Sprache „Incidents" heißen, Vorfälle. „Als global agierender ICT-Dienstleister mit Kunden sind wir auf zwei oder drei kritische Situationen pro Schicht eingerichtet." Dann ist es seine Aufgabe als Koordinator, schnellstmöglich den richtigen Löschspezialisten zu aktivieren. In diesem Augenblick, an einem Feiertag im Mai zum Beispiel. Der Notruf erreicht den Berliner zu Hause – mit Pizza in der Hand auf dem Weg zum Backofen. Doch noch bevor der Global Lead Incident Manager sein Arbeitszimmer erreicht, ist er per Telefon bereits informiert, „wo's brennt" – sechs Zeitzonen vor Deutschland.

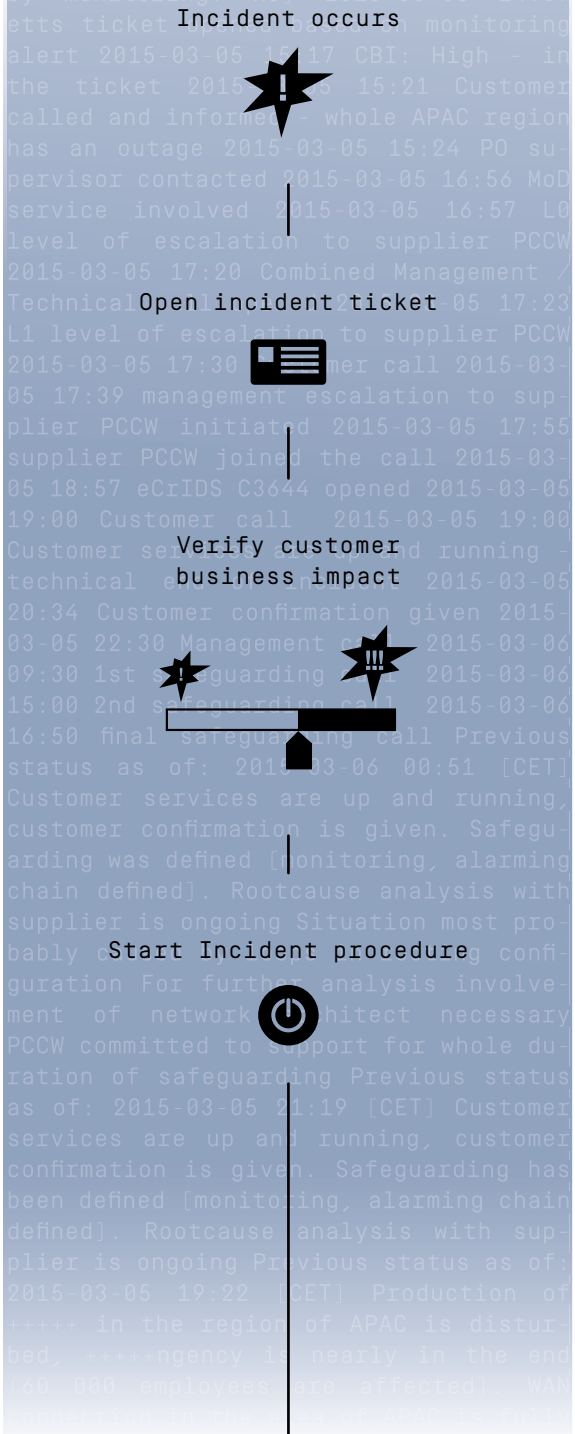
SINGAPUR, 16:57 UHR:
STILLSTAND FÜR 60 000 USER

„Major incident – outage of WAN network in APAC". Genau 20 Minuten „nach Alarm" bleiben Germersdorf, um den „1st combined technician management call" mit allen beteiligten Fraktionen aufzusetzen. Dem Service, der Delivery, der Technik zum Beispiel. Fortan steuert er sämtliche Deeskalationsmaßnahmen, hat die Einsatzverantwortung auf den Schultern und den Zeitdruck im Nacken. Von der ersten Sekunde an. Dafür stellt ihm jede potenziell betroffene Abteilung sofort einen MoD zur Incident-Behebung an die Seite.

Die Schadensbeschreibung des Global Incident Control Center, das den Notruf des Kunden angenommen hat, macht schnell klar: Hier geht's um etwas Großes. „Und vom ersten Moment an ist Adrenalin im Call", versichert Germersdorf: „WAN connection provided in Asia Pacific area is fully disrupted. Production of customer in the region of APAC is disturbed, affecting approximately 60 000 users." Stillstand für 60 000 Mitarbeiter ist aus Kundensicht ein Desaster. Und „Kundensicht ist immer unsere Sicht!" Nicht nur bei der fachlichen Beurteilung eines Incident, aber in Hinblick auf den „pressure", den der Vorfall für ein Unternehmen auslöst. Kein Wunder: Von einem halben Dutzend sofort eröffneter Tickets informiert Nr. 8760047 über den „real impact": „E-mail communication, web-traffic, financial processes, supply chain, operational processes, HR and production processes are all affected."

INCIDENT MANAGEMENT PROCESS

Jeder einzelne Schritt im Incident Management folgt festgelegten, vom TÜV Rheinland zertifizierten Prozessabläufen und wird von den weltweiten Teams bis zu 500-mal im Jahr trainiert.



Fortlaufend erhält der Lead Incident Manager Statusmeldungen der eingesetzten Techniker.

BERLIN, 11:22 UHR:
TEAM-BUILDING IN REKORDGESCHWINDIGKEIT

Bei „größeren Lagen“, also potenziell kritischen oder vom Kunden als kritisch eingestuften Incidents, kommen so schnell mal mehr als 20 Fachleute in diese Expertentelefonkonferenz, die ab jetzt die durchgehende Kommunikationsader zwischen allen Parteien darstellt. Die sind mitunter auf der ganzen Welt verteilt, und ihren Einsatz koordiniert der Global Lead Incident Manager im virtuellen War Room. Das betrifft nicht nur T-Systems‘ interne Kollegen, auch Managementvertreter von potenziell beteiligten Herstellern wie Cisco, Microsoft, VMware, SAP, F5 oder Juniper. Bei besonders kniffligen Situationen wird zusätzlich sofort ein Mitglied der T-Systems-Geschäftsführung hinzugezogen, denn kritische Ausfälle sind bei der Telekom-Tochter automatisch „Chefsache“. Dass Germersdorf und das Team direkten Zugriff auf die Daten der Technologiepartner haben und dort sofort Ansprechpartner bereitstehen, spart wertvolle Zeit. In der Incident-Sprache: meantime to repair. Die fixiert für jeden möglichen Incident die laut SLA verabredete maximale Reparaturdauer.

Sein „Call“ ist dabei das zentrale Instrument für die weltweite Zusammenarbeit. Er bleibt fortan permanent bestehen, alle 30 Minuten gibt es ein Status-Update. Bis irgendwann später endlich die Nachricht kommt, deren Eintreffen jeder einzelne Beteiligte mit seinem individuellen „know-how and talent“ betreibt: Customer services are up and running (technical end of the incident). Bis dahin, wiederholt Germersdorf, „bleibt der Call, denn ein Verantwortungs-Pingpong untereinander ist das Letzte, was wir in so einer Situation brauchen“.

Die Abläufe folgen einem festgelegten (und auch vom TÜV Rheinland zertifizierten) Prozess und sind von jedem MoD einstudiert und vielfach erprobt. „Training schärft die Sinne“, sagt Germersdorf. Unter der Bezeichnung „Fire Drills“ laufen bei T-Systems jährlich mehr als 500 Incident-Übungen ab – über die komplette Organisation. Von der Telefonannahme bis zum Executive. Und auch hier gilt: „Ob sich einer zu Hause gerade ein Brötchen schmiert oder mit der Familie unterm Weihnachtsbaum sitzt – wer Bereitschaft hat, lässt alles stehen und liegen, um sofort zu reagieren.“ Das heißt zunächst einmal, sprechfähig zu sein, gegenüber dem Kunden, seinem Accounter und den Technikern, die es zu steuern gilt. „Sprechfähig“ ist laut Germersdorf „der erste Schritte zur Deeskalation“. Schnell, strukturiert nach definierten Prozessketten und klaren KPIs, mit denen sich der Erfolg – oder Misserfolg – jeder eingeleiteten Maßnahme sofort kontrollieren lässt.

Fotos: Thorsten Futh

MAGDEBURG, 11:39 UHR:
SOFORT-CHECK AUF BEKANNTE MUSTER

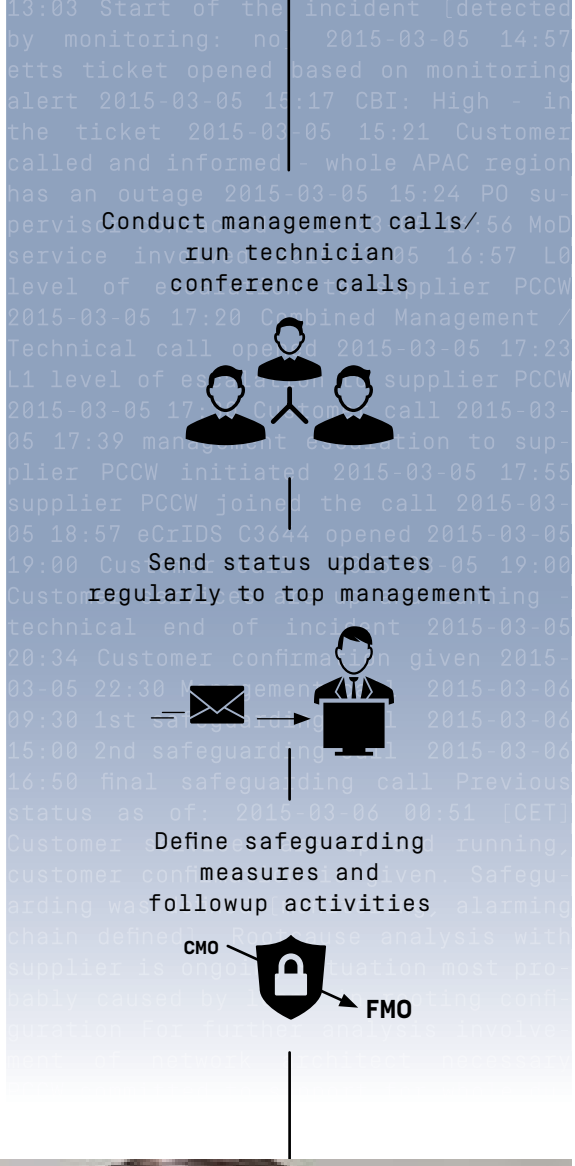
Eines der roten Telefone – quasi die Schaltzentralen von T-Systems für kritische Incidents – steht in Magdeburg. Und hier gilt jeder erste Blick sofort der Incident-Historie. Ist Vergleichbares schon einmal passiert? Wo sind die Muster? Könnte eine bewährte Lösung greifen? Ist dies nicht der Fall, starten die standardisierten Abläufe. „Wir überprüfen sofort, welche Standorte betroffen sind und was über die erste Schadensbeschreibung hinaus im schlimmstmöglichen Fall passiert sein kann. Diese Analysen laufen über die Technikverantwortlichen."

SINGAPUR, 18:01 UHR:
PARALLEL-CHECK MIT DEN TECHNIKERN

Parallel zum Management-Call führen Techniker verschiedenste Analysen für den betroffenen Kunden durch. Denn die Erstmeldung, „WAN des Kunden in großem Stil ausgefallen", heißt nicht: Damit ist der Suchradius für die Ursache des Fehlers abgesteckt. Im Gegenteil: Server, Betriebssysteme und Applikationen, der Datenbankbetrieb, das Netzwerk, selbst die Strom-Klima-Lage der Rechenzentren im Schadensgebiet – „parallel zum Call werden alle möglichen IT-Komponenten überprüft", stellt Germersdorf klar. Aber noch besteht kein Grund zum Aufatmen. Sein Laptop wird geflutet von kurzen technischen Statusmeldungen: — cn-cti-shang-cx-09 ping statistics — 5 packets transmitted, 0 received, 100% packet loss, time 4022ms.

Und auch dass diese Nachricht als Statusmeldung an den Kunden geht, ist Teil der Routine: „We would like to inform you that escalation of this case at a high level to our local partner is on track. The investigation of the incident is still ongoing, unfortunately, with no details regarding the time of the restoration available at the moment. As soon as we will have any news, we will inform you accordingly. Best regards." Höchste Priorität ist dabei immer, den Kunden während des gesamten Störungsmanagements nicht nur stets informiert zu halten, sondern ihn auch aktiv in die Risikoabwägung aller Lösungsoptionen einzubinden. „Bei kompletten Systemneustarts zum Beispiel entscheidet der Kunde, wann der geeignetste Zeitpunkt dafür ist."

Eines steht mittlerweile fest: Die Fehleranalyse wird mit der jüngsten Information schwieriger als gedacht. Doch mit jedem Check lichtet sich die IT-Nebelwand zusehends: Diesmal liegt die Ursache des Ausfalls tatsächlich „nur" in einer defekten WAN-Anbindung. „Nur", sagt Germersdorf gequält, „für 60 000 Mitarbeiter." Er weiß, was das bedeutet. Bis 2008 als Operator im Magdeburger Global Incident Control Team gehört der ausgebildete Fachinformatiker seit sieben Jahren zum Global MoD Service. Fieberhaft sucht sein „virtuelles" Team irgendwo im Bermudadreieck zwischen China, Malaysia und Australien nach dem Verursacher. Und mit jeder Minute wird die Fehlerursache weiter eingegrenzt. „Closed!", „Closed!", „Closed!" – per Mail melden die eingesetzten Spezialisten immer weitere „potential risks", die sich als Incident-Quelle ausschließen lassen. Dann der erste Durchbruch: Die Netzwerkexperten lokalisieren verschiedene ausgefallene Netzknoten. Als Ursache identifiziert das Team eine Dreiviertelstunde später zwei Router, von denen mindestens einer offenbar nicht mehr ordnungsgemäß arbeitet. „Jeder Netzwerkknoten für sich genommen war als ‚medium', also mittelkritisch, im System verzeichnet, so wie es der jeweiligen Niederlassung in der APAC-Region für den Kunden entsprach", erklärt Germersdorf in seiner ersten Atempause seit Stunden. „Aber wenn viele dieser als nur mittelkritisch eingestuften Komponenten gleichzeitig ausfallen, wird es natürlich zu einem extrem kritischen Incident. Da entwickeln sich fünf, sechs Strohfeuer schnell zu einem Flächenbrand."



Fotos: Thorsten Futh

CANBERRA, 21:50 UHR:
DIAGNOSEMELDUNG AN SERVICEPARTNER

Das Incident Management über acht Zeitzonen hinweg ist abgeschlossen. Es war der Router eines Kundenstandorts im australischen Canberra. Der instruierte Servicepartner vor Ort hat den Schaden innerhalb einer Stunde behoben. Die Fachleute verkünden im Call die technische Diagnose: „It was discovered that there was an incorrect, or risky configuration command entered on the router that was causing a flapping of the connection with other autonomous systems. A Network Protocol was flapping on the local internet access line consequently lead to the flapping routes on the NNI (Network to Network Interface).“ Auf Deutsch: Infolge eines unkontrollierten Umschaltens in der Aktiv-/Passiv-Konfiguration der zwei redundanten Router war der Netzknoten für 60 000 Mitarbeiter nicht mehr erreichbar, und so war die Konzernkommunikation des Kunden in der gesamten APAC-Region gestört. Schon ein winziges Steinchen auf dem Modul der Lichtleiterverbindung zwischen den Routern kann solch einen unangekündigten Hardwarefehler auslösen.

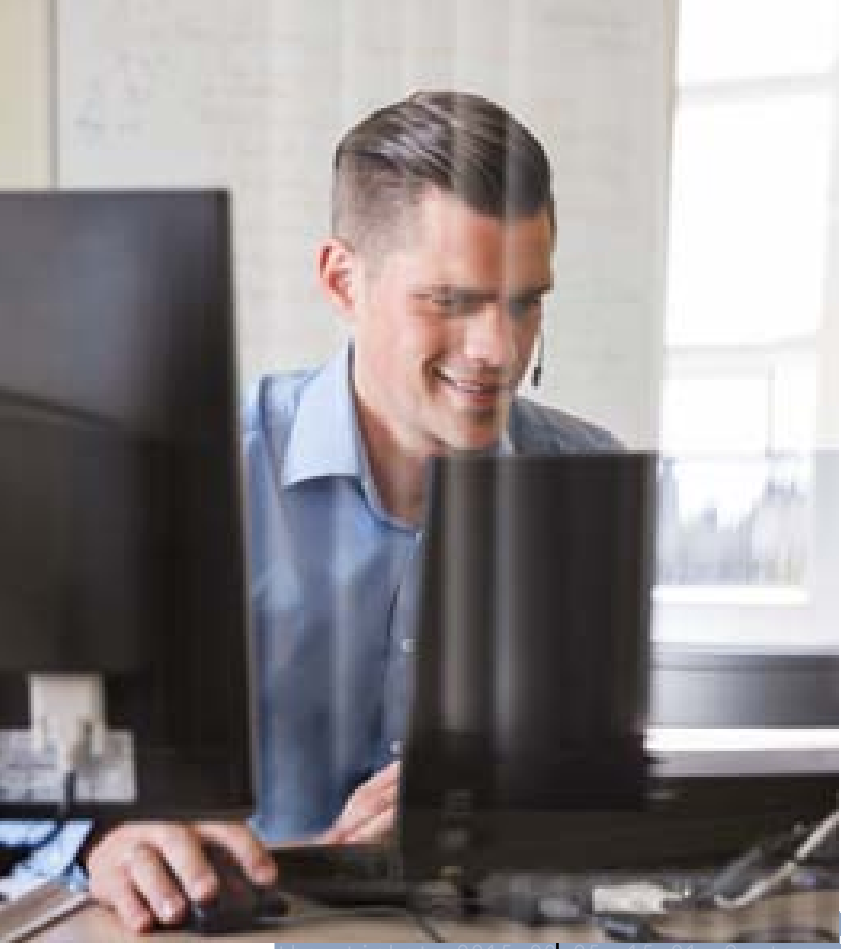
Die exakte Fehleranalyse durch den Hersteller wird später als Teil der Incident-Nachbearbeitung den entsprechenden Patch liefern. Doch um die Folgen so einer Funktionsstörung in Zukunft zu minimieren, hat der Lead Problem Manager, an den Germersdorf die Nachbearbeitung des Incident übergeben wird, auch eine Konzeptänderung auf Lager, zu der das Serviceteam dem Kunden für die Zukunft raten wird: Um auch unvorhersehbare Lücken auszuschließen zwischen dem SLA, das Kunden zum Initial Design ihrer Architektur anfordern, und dem Servicelevel, das aus T-Systems-Sicht prozesstechnisch erforderlich wäre, so Germersdorf, „werden wir dem Kunden empfehlen, den als ‚medium‘ eingestuften Netzknoten auf ‚critical‘ upzugraden“.

MAJOR INCIDENT = HIGH MANAGEMENT ATTENTION

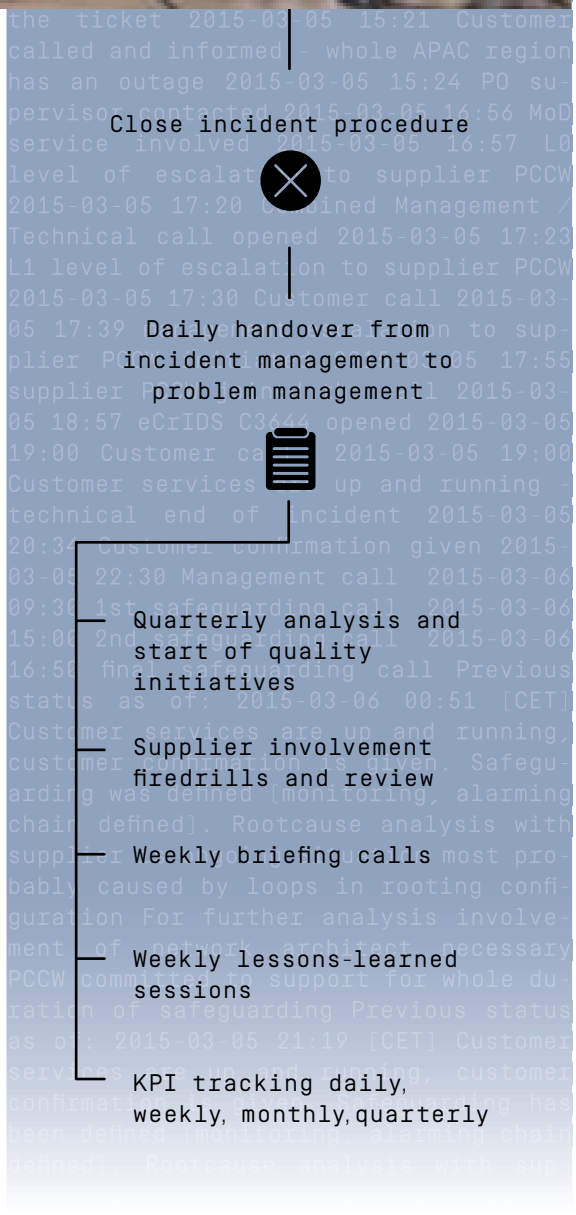
„Bei uns gilt: Major Incident = High Management Attention. Das ist der Unterschied zu unserem Wettbewerb. Die gesamte Executive-Ebene und sämtliche Senior Vice Presidents sind 24/7 über jedes Status-Update informiert. Das prägt jeden Einzelnen im ganzen Konzern, ist Teil unserer DNA und lenkt den Fokus automatisch viel stärker auf unsere Kunden. Jeder Senior Vice President ist Manager-on-Duty, alle Board Member sind informiert, und bei ganz kritischen Situationen haben unsere Kunden direkten und sofortigen Zugriff auf die T-Systems-Geschäftsführung. Auch am Wochenende. Das ist gelebte Kundennähe – Zero Distance. In meinen 28 Jahren in der IT-Industrie kenne ich das von keinem anderen Provider.“

Carsten Gram,
Senior Vice President Big Deal Management, T-Systems

Automatisch werden alle vom Kunden eingesetzten Configuration Items (Betriebsmittel) weltweit gemonitort.



Entspanntes Lächeln – erst mit der Statusmeldung „Customer services are up and running" lässt der mitunter stundenlange Hochdruck im Team nach.



BERLIN, 16:51 UHR:
PLAN B IN DER SCHUBLADE

Geübt oder nicht – mitunter heiße es auch bei noch so oft trainierten Abläufen „einfach improvisieren", so Germersdorf. Denn die Bandbreite externer „Funktionsstörer" kann vom kleinen Stein, wie heute in Australien, bis zum 2000 Meter hohen Brocken reichen. Wenn etwa am anderen Ende der Welt Esja, Katla oder Eyjafjallajökull allen Alarmplänen einen Strich durch die Rechnung machen.

Erst im vergangenen Jahr war es Bardarbunga, einer von 31 isländischen Vulkanen, der große Teile des europäischen Flugverkehrs lahmlegte. Wie der Incident eines schwedischen Kunden zu beheben sein würde, hatte der Global MoD Service am selben Tag rasch ermittelt. Das nötige Serverersatzteil von einem Sub-Provider des Unternehmens war in den Niederlanden schnell beschafft. Doch dann saß der Techniker am Flughafen Amsterdam fest. „Quasi mit dem Ersatzteil auf dem Schoß", erinnert sich Germersdorf, „und es war klar, in halb Europa würde tagelang kein Flugzeug starten. Hier wurden ruck, zuck die Zollpapiere organisiert, das Ersatzteil per Kurier mit Lkw und Fähre nach Stockholm gebracht." In einem anderen Fall war die Lage so brenzlig, dass ein Softwareexperte per Helikopter eingeflogen werden musste. Auch dieser Aufwand hat sich am Ende für den Kunden gerechnet.

„Wir versuchen, aus jedem Vorfall Lehren zu ziehen", so Stephan Kasulke, Senior Vice President Quality bei T-Systems, „um die Ausfallsicherheit bei unseren Kunden ständig zu steigern" (siehe Interview Seite 31). So führen die Erkenntnisse aus echten Incidents und „Fire Drills" nicht nur zu einer immer weiteren Verfeinerung der Krisenmanagementprozesse, sondern auch zu einer deutlich besseren Vorhersage drohender IT-Ausfälle. Beispiel Configuration Items: „Alle sogenannten CIs, die vom Kunden eingesetzten IT-Betriebsmittel wie Server, Software oder Netzwerke, sind bei uns im Monitoring", erklärt Germersdorf. „Im Idealfall sehen wir so frühzeitig, wo welche Kundenapplikationen unsauber laufen, ob ein Server betroffen ist, der für 50 Kunden arbeitet, oder fünf Server, die ausschließlich für ein Unternehmen Dienst tun."

BERLIN, 17:10 UHR:
END OF INCIDENT

Die Betreffzeile der finalen E-Mail entfaltet die Stirn des Lead Incident Managers sichtlich. „End of Incident" heißt für Germersdorf: „meantime to repair" eingehalten – und für den Kunden: Alle 60 000 User können wieder vernünftig arbeiten. Für Steffen Germersdorf bedeutet die Mail: Fall abgeschlossen und „erst mal aufstehen" – vom Schreibtisch im heimischen Arbeitszimmer. In der Küche eines IT-Experten sind lebenswichtige Komponenten zum Glück auch redundant ausgelegt. So findet Germersdorf im Kühlfach heute Abend noch eine „Backup-Pizza", die er sich – im wahrsten Sinne des Wortes – „redlich" verdient hat.

‹Kontakt› *stephan.kasulke@t-systems.com*
‹Link› *t-systems.de/zero-outage*